

SEYFARTH SHAW LLP Kevin J. Mahoney (SBN 6299398) ( <i>pro hac vice pending</i> ) kmahoney@seyfarth.com 233 South Wacker Drive Suite 8000 Chicago, Illinois 60606-6448 Telephone: (312) 460-5000 Facsimile: (312) 460-7000  Mark. A. Wagner (UT 06353) mawagner@seyfarth.com 975 F St., N.W. Washington, DC 20004 Telephone: (415) 732-1152  Attorneys for Plaintiff Bill.com, LLC	
---	--

UNITED STATES DISTRICT COURT  
DISTRICT OF UTAH - CENTRAL DIVISION

Bill.com, LLC,  Plaintiff,  v.  Danielle Cox,  Defendant.	<p style="text-align: center;"><b>PLAINTIFF’S EMERGENCY MOTION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION AND SUPPORTING MEMORANDUM</b></p> <p>Case No. 2:23-cv-00026-JNP</p> <p>Hon. Jill N. Parrish</p>
---	---

Plaintiff Bill.com, LLC (“BILL”), by and through its counsel and pursuant to Federal Rule of Civil Procedure 65, respectfully moves this Court for a Temporary Restraining Order and Preliminary Injunction. Specifically, BILL seeks temporary and preliminary injunctive relief against Defendant Danielle Cox’s (“Defendant” or “Cox”) unlawful use and threatened disclosure

of BILL's confidential and trade secret information. Specifically, BILL seeks an order directing Cox to return BILL's company-issued computer, to cease any use or disclosure of BILL's confidential and trade secret information in her possession, to return such data to BILL in a manner that preserves all relevant metadata, and to refrain from destroying any relevant evidence. In support thereof, BILL submits the following Memorandum in support of its Motion.

## **I. INTRODUCTION**

BILL provides cloud-based financial services—Cox is the former Director of Information Technology in BILL's Information Technology ("IT") Group. Cox began a requested leave from BILL on December 5, 2022. The Friday before that leave began, December 2, 2022, Cox used her enhanced administrator credentials at BILL in order to download nearly **5,800** emails from the inbox of her direct supervisor. Cox then synced that data with an unauthorized, cloud-based account. Over the next two weeks, even after her leave began, Cox continued to use her administrator-level access to access and search the email accounts of other BILL employees, without any authorization or possible legitimate purpose. Cox also exported the entire internal messaging logs of **every** BILL employee for a months-long period, and BILL's forensics investigation indicates that she may have used a non-company computer to do so. The data that Cox exfiltrated includes some of BILL's most sensitive confidential and trade secret information regarding its operations and ongoing business plans and strategies.

BILL discovered Cox's actions on December 19, 2022 and immediately suspended her access to its networks. Between December 21, 2022 and January 9, 2023, BILL reached out to Cox well over a half-dozen times, via text message, phone calls, emails, and correspondence sent via overnight courier, to demand an explanation for her actions and the return of its company-issued

computer and data. Cox ignored every attempt at communication, and refuses to return BILL's computer. As a result of her actions, BILL terminated Cox on January 9, 2023. That same day, a BILL representative reached Cox by phone and explained that the company would seek legal action immediately if she continued to ignore its requests. Despite that final warning, Cox continues to ignore BILL's requests for the return of its information and equipment. Every day that goes by that Cox refuses to return BILL's data and equipment, and refuses to confirm that she has not improperly used or disclosed that data, puts BILL's confidential and trade secret information at significant risk of disclosure and misuse.

The relief that BILL seeks through this Motion is limited: all that BILL requests is an injunction against Cox's use or disclosure of BILL's information, the return of its computer equipment, the return of its data in a manner that preserves relevant metadata, and an order directing Cox to preserve evidence. Cox's ongoing refusal to return BILL's confidential and trade secret information or its computer equipment has made it clear that injunctive relief is necessary to enforce BILL's contractual rights, as well as its rights to its confidential and trade secret information under state and federal law. For all the reasons set forth below, BILL's motion should be granted.

## **II. FACTUAL BACKGROUND**

### *BILL's Business and Cox's Role*

BILL was founded in 2006 as a provider of automated, cloud-based software for financial operations and end-to-end payments. (*See* Declaration of Steven Januario attached hereto as Exhibit A ¶ 3.) Over the last 16 years and through several acquisitions as well as organic growth, BILL has grown into a leading provider of cloud-based financial operations software to tens of

thousands of other businesses. (*Id.*) BILL's operations are dependent upon the safety and security of its electronic information and data systems. (*Id.* ¶ 4.) BILL has spent nearly two decades developing proprietary and confidential information about its personnel, operations, business plans and strategies, and marketing plans. (*Id.*) Because of the sensitivity of that information, along with the sensitivity of the financial information that BILL's customers entrust to it, BILL invests significant amounts of time and money into its physical computing systems, as well as the personnel who maintain BILL's networks and information. (*Id.*)

On or about March 11, 2019, Defendant Cox joined DivvyPay, Inc., a provider of expense management software to other businesses, as an IT Manager. (*See* Declaration of Alisa Lewis attached hereto as Exhibit B at ¶ 3.) DivvyPay, Inc. was later acquired by BILL in May of 2021 and Cox continued her employment with BILL as a Director of Information Technology in BILL's IT group. (*Id.*) As a Director of Information Technology in BILL's IT group, Cox was given enhanced access and credentials to BILL's electronic systems. (Ex. A ¶ 5.) Specifically, in order to effectively accomplish her duties as one of the leaders of BILL's IT group, Cox was given "super administrator" credentials that allowed her to access virtually all of BILL's systems and information, including the email accounts of other employees. (*See* Declaration of Robert Blenkinsop attached hereto as Exhibit C ¶ 3.) Simply put, by virtue of her enhanced credentials, Cox had direct access to the information that drives BILL's success as an organization, and specifically with regard to information about its ongoing operations and business plans. (*Id.*; (Ex. A ¶ 5.)

### *BILL's Protection of Its Confidential Information and Trade Secrets*

Because of the critical nature of BILL's confidential and trade secret information and how it allows BILL to succeed, BILL closely guards its confidential information and trade secrets. (Ex. A ¶ 6.) BILL takes specific measures to restrict access to and preserve the confidentiality of this information, including, but not limited to, the following:

- a. Requiring its employees to sign agreements containing covenants designed to maintain confidentiality and to return BILL property upon termination of their employment with BILL;
- b. Prohibiting its employees from using, copying, divulging, or otherwise disseminating or disclosing BILL confidential information outside of BILL;
- c. Restricting access to BILL confidential information on a "need to know" basis;
- d. Requiring employees with access to BILL's systems to acknowledge and agree to adhere to policies regarding the use of that information, including but not limited to an Acceptable Use Policy;
- e. Requiring employees to access BILL's systems using secure Virtual Private Network connections; and
- f. Requiring employees to use unique login credentials and passwords to access BILL's confidential information.

(*Id.*) BILL rigorously maintains the confidentiality of its information because the information provides BILL a competitive advantage in the marketplace from which it derives economic value.

(*Id.* ¶ 7.) Any BILL competitor who improperly possessed and used this confidential information, particularly about BILL's operations and business plans, would gain an immediate and unfair competitive advantage, and would be able to unfairly compete with BILL. (*Id.*) While BILL's information is primarily generated from its headquarters in California, that information is available

to its employees across the nation, including to Ms. Cox from her work location in Utah (Ex. C ¶ 4.)

*Cox's Contractual Obligations to BILL*

When Cox joined DivvyPay, Inc., and as a condition of her employment and before being given access to any confidential information, she was required to enter into a Proprietary Information and Inventions Agreement, dated February 27, 2019. (Ex. B ¶ 4.) Later, and again as a condition of her ongoing at-will employment and continuing access to confidential information, Cox was required to enter into an updated Proprietary Information and Inventions Agreement dated October 9, 2019 (“the Agreement”). (*Id.*) When BILL acquired DivvyPay, Inc. in May of 2021, DivvyPay, Inc.’s rights under the Agreement were assumed by BILL as a matter of law in connection with that acquisition. (*Id.* ¶ 5.) At the same time, Cox acknowledged that the Agreement would remain effective after the acquisition was complete. (*Id.*)

The Agreement contains certain restrictions on Cox’s activities while she was employed by BILL and after, along with restrictions on Cox’s use of BILL’s confidential and trade secret information. (*Id.* ¶ 6.) In the Agreement, Cox acknowledged that she was being given access to valuable proprietary information, defined in the Agreement as:

“information owned by the Company or licensed from third parties regarding (a) research, development, products, services, marketing, selling, business plans, budgets, unpublished financial statements, licenses, prices, costs, contracts and other agreements, suppliers, customers, and customer lists; (b) the identity, skills and compensation of employees, contractors, and consultants; (c) specialized training; and (d) information related to Inventions owned by the Company or licensed from third parties.”

(*Id.*)

With regard to that confidential information, Cox acknowledged and agreed that:

“...during my Service and thereafter, pursuant to this agreement, I will hold in strictest confidence and will not disclose, discuss, transmit, use, lecture upon, or publish any Proprietary Information, except as such disclosure, discussion, transmission, use, or publication may be required in connection with my Service, or unless the Chief Executive Officer or Board of Directors of the Company expressly authorizes such disclosure in writing.”

(*Id.* ¶ 7.) Cox further agreed that if her employment ever ended, she would return all property of the company, “including but not limited to laptops, pagers, cell phones, corporate credit cards, keys and/or access cards.” Cox also agreed that such property of the company was subject to inspection at any time, with or without notice. (*Id.* ¶ 8.)

In addition to her obligations under the Agreement, Cox also agreed to BILL’s Acceptable Use Policy. (*Id.* ¶ 9.) BILL’s Acceptable Use Policy, which Cox was tasked with implementing as a member of IT leadership, mandates that any confidential information stored on BILL’s electronic and computing devices is the sole property of BILL, that Cox had an obligation to report any unauthorized use of such information, that she was permitted to access such information only to the extent it was authorized and necessary to fulfill her assigned job duties, and that she was strictly prohibited from syncing personal iCloud or other cloud-based accounts to company-issued devices. (Ex. C ¶ 5.) The Acceptable Use Policy further prohibits Cox from using other employee’s accounts, from taking any actions to “disable, damage or otherwise interfere with any security related features,” or from attempting to gain unauthorized access to BILL’s accounts. (*Id.* ¶ 6.)

Cox agreed that the Agreement would be governed by and construed in accordance with the law of the State of Utah. (Ex. B at ¶ 10.) Cox also agreed that in any action to enforce the confidentiality restrictions in the Agreement, injunctive and equitable relief would be appropriate without the necessity of posting a bond, and such an action should be tried and litigated in the state or federal courts of Utah. (*Id.*) Cox also agreed in her Offer Letter agreement with DivvyPay, Inc.

that, except for actions seeking injunctive relief as a result of her breach of the Agreement, any dispute arising from her employment would be subject to binding arbitration. (*Id.* ¶ 11.) Those rights were also assumed by BILL as a matter of law in connection with the acquisition of DivvyPay, Inc. (*Id.*)

#### *Defendant Cox Breaches Her Agreement*

On or about November 30, 2022, Cox requested a leave of absence from BILL. (*Id.* ¶ 12.) That request was granted and Cox's leave was to begin on Monday, December 5, 2022. (*Id.*) On December 2, 2022—the Friday before her leave was scheduled to begin—Cox used her enhanced credentials to access BILL's electronic systems, including its Google Vault application. (Ex. C ¶ 7-10.) Using those enhanced credentials to the company's Google Vault, Cox accessed and downloaded nearly **5,800** emails from the inbox of her direct supervisor. (*Id.* ¶ 10.) Those emails include highly sensitive, confidential, and trade secret information regarding BILL's personnel, operations, business plans and strategies, and marketing plans, along with privileged attorney-client communications regarding other matters involving the company. (Ex. A ¶ 8.) After she accessed those materials, Cox synced them from her company-issued computer to an unauthorized iCloud account. (Ex. C ¶ 11.)

Between November 30, 2022 and December 7, 2022, again using her enhanced credentials, Cox requested five different exports of data from BILL's corporate Slack account, including a manual export of the company's entire Slack database; *i.e.* the internal messaging of every employee of the company. (*Id.* ¶ 12-13.) Because BILL expected Cox to return from leave, it did not turn off her access to the company's systems or require the return of her company-issued computer while she was on leave. (*Id.* ¶ 15.) Between December 5, 2022 and December 20, 2022,



after her leave began, Cox continued to search for highly sensitive information of BILL in the email accounts of her direct supervisor and other colleagues. (*Id.* ¶ 14; Ex. A ¶ 8.) There is no legitimate reason why Cox needed to access, download, and exfiltrate any of the foregoing materials as part of her job duties, nor was she ever authorized to do so by anyone at BILL, much less while she was on leave. (Ex. A ¶ 10.)

Just days ago, BILL also discovered that in an apparent effort to hide her unauthorized access and exfiltration of the above-mentioned information, Cox altered the email retention settings on her email account (along with those of several other IT group members) such that deleted emails would be permanently destroyed after one day and rendered unrecoverable, rather than indefinitely retained per the prior setting. (Ex. C ¶ 17-18.) In a further apparent attempt to hide her actions, Cox changed these retention settings on her last day in the office before her leave was to begin (December 2), then changed the retention settings back to the default setting the following Monday (on December 5): *after* any emails she deleted would have been permanently destroyed. (*Id.* ¶ 19-20.)

On December 21, 2022, BILL investigated and discovered the extent of Cox's aforementioned access and downloading of emails and the company's Slack account and immediately suspended her access to the company's networks. (*Id.* ¶ 15.) The next day, BILL representatives began attempting to contact Cox by phone, text message, and email to her personal email account to request an explanation of her actions, as well as the immediate return of BILL's company-issued computer and any data belonging to the company. (Ex. B ¶ 13-14.) Cox ignored every attempt at communication. (*Id.*) On December 29, 2022, BILL sent cease and desist correspondence to Cox, both through her personal email and at her home, demanding that she

immediately return BILL's equipment and data, and that she confirm that the information she exfiltrated was not being shared or disclosed with any other third party. (*Id.* ¶ 15.) Again, Cox ignored that communication. (*Id.*)

As a result of her refusal to return the Company's property or explain her actions, BILL terminated Cox as an employee effective January 9, 2023. (*Id.* ¶ 16.) That same day, a BILL representative spoke to Cox telephonically and told her that the company would pursue legal action if she continued to ignore its demands for the return of its equipment and data. (*Id.*) As of the filing of this lawsuit, Cox continues to ignore BILL's attempts to reach her and refuses to return her company-issued computer or the materials that she wrongfully exfiltrated. (*Id.*) Cox clearly has no intention of returning BILL's confidential and trade secret information, and continues to ignore BILL's repeated demands for its return. It is apparent that Cox can be compelled only by this Court to abide by her contractual obligations as well as state and federal law, and return BILL's equipment and confidential and trade secret information.

#### *Effect of the Defendant's Conduct*

Because of Cox's intimate knowledge of BILL's electronic systems and data, Cox is uniquely positioned to cause BILL substantial harm through the misuse of BILL's confidential and trade secret information. (Ex. A ¶ 11.) Cox's use and threatened disclosure of BILL's confidential and trade secret information places BILL's goodwill, customer relationships, trade secrets, and confidential and proprietary information at significant risk of destruction or loss, which cannot be adequately addressed at law. (*Id.* ¶ 12.) Simply put, Cox's actions have already irreparably harmed, and will continue to irreparably harm, the value of BILL's confidential and trade secret information. (*Id.*)

### **III. ARGUMENT**

A temporary restraining order and a preliminary injunction should issue where a plaintiff demonstrates that (1) it has a substantial likelihood of prevailing on the merits; (2) it will suffer irreparable injury if the injunction is denied; (3) its threatened injury outweighs the injury that the opposing party will suffer under the injunction; and (4) an injunction would not be adverse to the public interest. *See Limitless Worldwide, LLC v. AdvoCare Int'l, LP*, 926 F. Supp. 2d 1248, 1250 (D. Utah 2013); *Stevens v. Ocwen Fed. Bank FSB*, No. 2:06-CV-397 TS, 2006 WL 1409139, at \*1 (D. Utah May 17, 2006) (“The standard for granting a TRO is the same as that for a preliminary injunction ....”). Courts have inherent authority to enter temporary restraining orders “to preserve the status quo pending a final determination of the rights of the parties,’ in order ‘to preserve the power to render a meaningful decision on the merits.’” *Resolution Tr. Corp. v. Cruce*, 972 F.2d 1195, 1198 (10th Cir. 1992) (quoting *Lundgrin v. Claytor*, 619 F.2d 61, 63 (10th Cir. 1980); *Tri-State Generation & Transmission Ass’n, Inc. v. Shoshone River Power, Inc.*, 805 F.2d 351, 355 (10th Cir. 1986).

In this instance, BILL can clearly establish that it is entitled to the limited relief that it seeks. BILL is very likely to succeed on the merits of its claims, and all that BILL is requesting is the return of information and computer equipment that indisputably belongs to BILL and not Cox, along with an order that Cox should not use or disclose such information and preserve relevant evidence. It is just as clear that BILL’s need for emergency injunctive relief is significant: despite repeated demands and several opportunities to resolve this issue short of litigation, Cox has steadfastly refused to return BILL’s information or equipment, or even confirm that she has not disclosed and will not disclose that information to unauthorized third parties. Compared to the

significant threat of irreparable harm facing BILL through the loss of its confidential information and trade secrets, Cox faces absolutely no harm whatsoever from the requested injunction, considering that the only relief that BILL seeks, again, is the return of equipment and data that does not belong to Cox and an order directing her not to use that information or destroy evidence. Finally, the public interest would be served by the protection of trade secrets and enforcement of the confidentiality restrictions in the Agreement. BILL's Motion should be granted.

**A. BILL Is Substantially Likely to Prevail on the Merits of its Claims for Trade Secret Misappropriation, Breach of Contract, and Conversion.**

“In applying Rule 65, the Tenth Circuit has recognized both (1) a ‘relaxed’ standard and (2) a ‘heightened’ standard. Where a movant establishes that the factors dealing with irreparable injury, the balancing of potential harms, and the potential harm to public interest ‘tip decidedly in its favor,’ the ‘probability of success requirement’ is somewhat relaxed.” *Navajo Nation Hum. Rts. Comm'n v. San Juan Cnty.*, 215 F. Supp. 3d 1201, 1207 (D. Utah 2016). Here, considering the clear risk of irreparable injury, the significant harm faced by BILL absent injunctive relief versus the nonexistent harm facing Cox, and the public interest favoring the granting of the requested injunction, the “relaxed” standard should apply to BILL's Motion. Under either standard, however, BILL can more than show “a reasonable probability that it will ultimately be entitled to the relief sought” on its claims, including its claims for violations of the Federal Defend Trade Secrets Act (18 U.S.C. § 1836 *et seq.*, “the DTSA”), the Utah Uniform Trade Secrets Act (Utah Code 13-24-1 *et seq.*, “the UTSA”), breach of contract, and conversion. *Crowther v. Seaborg*, 415 F.2d 437, 439 (10th Cir. 1969).

**1. BILL Is Likely to Succeed on the Merits of its Claim for Trade Secret Misappropriation.**

BILL is significantly likely to succeed on its claims for trade secret misappropriation against Cox. To establish misappropriation of trade secrets, the same basic elements must be shown under both the DTSA and UTSA: BILL must show that “(1) it possessed a protectable trade secret, (2) [Cox] misappropriated one or more of [BILL’s] trade secrets, and (3) [BILL] was damaged by [Cox’s] use of the secret.” *Surgenex, LLC v. Predictive Therapeutics, LLC*, 462 F. Supp. 3d 1160, 1170 (D. Utah 2020), on reconsideration in part, No. 2:19-CV-295-RJS-DAO, 2020 WL 8514831 (D. Utah July 17, 2020); *see also* 18 U.S.C. §§ 1836, 1839; Utah Code 13-24-2. Under both the DTSA and UTSA, this Court is empowered to grant an injunction to prevent an “actual or threatened misappropriation.” 18 U.S.C. § 1836(b)(3)(A)(i); Utah Code 13-24-3(1).

There is no reasonable dispute that the information Cox exfiltrated from BILL and refuses to return qualifies as trade secrets. Included among the 5,800 emails that Cox downloaded from her supervisor’s account are BILL’s highly sensitive, confidential, and trade secret information regarding its personnel, operations, business plans and strategies, and marketing plans, along with privileged attorney-client communications regarding other matters involving the company. (Ex. A ¶ 8.) Included among the Slack database information that Cox exported is confidential and trade secret information concerning nearly every facet of BILL’s business for a four-month period, from every single employee of the company. (*Id.* ¶ 9.) All of this information is subject to extensive efforts by BILL to protect it from public disclosure, and is non-public information from which BILL derives significant economic value. (*Id.* ¶ 7.) Moreover, all of this information falls squarely within the definition of trade secrets under both the DTSA and UTSA. *See* 18 U.S.C. § 1839 (“the term ‘trade secret’ means all forms and types of financial, business...information,

including...plans...); Utah Code 13-24-2 (“trade secret” means information...that derives independent economic value, actual or potential, from not being general known...; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”)

Beyond the existence of its trade secrets, it is also clear that BILL can establish that Cox misappropriated those trade secrets. The DTSA and UTSA both define “misappropriation” as the “acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.” 18 U.S.C. § 1839(5)(A); Utah Code 13-24-2(2). The term “improper” includes “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.” 18 U.S.C. § 1839(6)(A); Utah Code 13-24-2(1). Here, Cox violated the Agreement and BILL’s Acceptable Use Policy , and misused her enhanced credentials, in order to access and download thousands of emails from the account of her supervisor, and to sync that information with an unauthorized iCloud account. Utah courts have recognized nearly analogous situations, where an employee with nominal “access” to information exfiltrates it to an unauthorized account or refuses to return it, as misappropriation of trade secrets. *See InnoSys, Inc. v. Mercer*, 2015 UT 80, ¶ 27 (employee’s forwarding of trade secrets from a secure company computer system to personal email account just prior to termination “at least arguably amounts to misappropriation by unlawful disclosure” under UTSA).

As to the last element, and as explained further below, it is black letter law that the loss of BILL’s trade secrets would not just *damage* BILL, but would amount to irreparable harm that “cannot be measured in money damages.” *Id.* at ¶ 73; *Paparazzi, LLC v. Sorenson*, No. 4:22-CV-00028-DN, 2022 WL 1469459, at \*3 (D. Utah May 10, 2022) (“Without a temporary restraining

order protecting Paparazzi's Confidential Information, Paparazzi is likely to suffer irreparable harm that cannot easily be reduced to monetary damages.”) Particularly in this situation, where Cox is uniquely situated to use BILL’s trade secrets to injure BILL’s goodwill, standing with its customers, and the value of its trade secret information, the irreparable harm to BILL in the absence of injunctive relief is all but assured. (Ex. A ¶ 11-12.) Cox not only abused her position at BILL to exfiltrate its trade secrets, she now flatly refuses to confirm that she is not actively using or disclosing those trade secrets to unauthorized third parties. Under those circumstances, BILL is more than likely to succeed on the merits of its claims for trade secret misappropriation,

**2. BILL is Likely to Succeed on its Breach of Contract Claim.**

BILL is also likely to succeed on its breach of contract claims. “The elements of a prima facie case for breach of contract are (1) a contract, (2) performance by the party seeking recovery, (3) breach of the contract by the other party, and (4) damages.” *Mint Solar, LLC v. Savage*, No. 2:18-CV-569 TS-PMW, 2018 WL 5924410, at \*3 (D. Utah Nov. 13, 2018), *on reconsideration*, No. 2:18-CV-569 TS, 2018 WL 6602213 (D. Utah Dec. 17, 2018).

Here, the only provisions of the Agreement that BILL seeks to enforce are the prohibition against Cox’s use or disclosure of BILL’s information, and her obligation to return BILL’s equipment to it.<sup>1</sup> Such non-disclosure restrictions are routinely enforced under Utah law and should be enforced here. *See Paparazzi, LLC*, 2022 WL 1469459, at \*2 (“The Confidentiality Agreement is a valid and binding contract between Paparazzi and Defendant Sorenson. The Confidentiality Agreement required Sorenson to keep Paparazzi's Confidential Information strictly

---

<sup>1</sup> Cox’s Agreement also contains post-employment restrictions in the form of non-compete and non-solicit terms. To be clear, BILL is not seeking to enforce those provisions at this time - the only issue is Cox’s refusal to return BILL’s equipment and data.

confidential” and granting injunctive relief based on same.”); *Envirotech Corp. v. Callahan*, 872 P.2d 487, 495 (Utah Ct. App. 1994) (enforcing agreement that simply required defendant employee not to divulge confidential or proprietary information of employer and, after termination, to return any material belonging to employer). BILL performed all of its obligations under the Agreement by providing Cox continuing access to confidential information (Ex. A ¶ 5), and there is no dispute that Cox breached, and continues to breach, the Agreement by failing to return BILL’s property to it, causing BILL damage in the loss of its data and computer, as well as the ongoing exposure of BILL’s trade secrets and other confidential information to unauthorized parties (including Cox herself, who is no longer an employee of BILL). (Ex. B ¶ 13-16, Ex. C ¶ 2178). Again, there is little doubt that BILL will succeed on the merits of its breach of contract claim considering that Cox has absolutely no right to possess the information or equipment in question, and BILL easily satisfies both the relaxed and heightened standards for a likelihood of success showing on that claim.

### **3. BILL Is Likely to Succeed on its Conversion Claim.**

Lastly, BILL is also likely to succeed on its claim for conversion of the computer that it issued to Cox. “To prove conversion, a party must establish ‘an act of willful interference with property, done without lawful justification, by which the person entitled to property is deprived of its use and possession,’ and that the party ‘is entitled to immediate possession of the property at the time of the alleged conversion.’” *Jones & Trevor Mktg., Inc. v. Lowry*, 2010 UT App 113, 233 n.13, *aff’d*, 2012 UT 39. The computer that BILL issued to Cox is BILL’s property, which Cox agreed to return upon BILL’s demand for same, and in any event to return at the end of her employment. (Ex. C ¶ 21; Ex. B ¶ 8.) Despite BILL’s right to immediate possession of that



property, Cox refuses to return that equipment and has ignored every one of BILL's repeated requests for the return of that equipment over the past several weeks. (Ex. B ¶ 13-16.) There is no lawful justification for Cox's refusal to return BILL's equipment, and BILL is likely to succeed on its claim for conversion for all of those reasons.

**B. BILL Will Suffer Irreparable Injury Without Injunctive Relief.**

BILL will undoubtedly suffer irreparable harm in the absence of the requested injunctive relief. Irreparable harm occurs when the injury that will result without the injunction cannot adequately be compensated by damages or a trial on the merits. *Tri-State Generation*, 805 F.2d at 355; *RoDa Drilling Co. v. Siegal*, 552 F.3d 1203, 1210 (10th Cir. 2009). The Utah Supreme Court has recognized that there is a presumption of irreparable harm in the case of trade secret misappropriation. *InnoSys, Inc. v. Mercer*, 364 P.3d 1013 (Utah 2015) (a "long-settled principle of trade secret law recognizes a presumption of harm upon proof of misappropriation"); *Bimbo Bakeries USA, Inc. v. Sycamore*, No. 2:13-CV-00749-DN-DBP, 2018 WL 1578115, at \*5 (D. Utah Mar. 29, 2018) ("Under the UTSA, there is a presumption of irreparable harm where trade secret misappropriation is found. The presumption is rebuttable if a defendant can show a trade secret no longer exists, but a plaintiff need not prove economic harm or the likelihood of additional disclosures."). "The presumption of irreparable harm is rebuttable *only* based on a showing that the trade secret no longer exists." *Gatti v. Granger Med. Clinic, P.C.*, 529 F. Supp. 3d 1242, 1268 (D. Utah 2021) (emphasis added).

Even without the *presumption* of irreparable harm, it is clear from the supporting declarations that BILL faces significant, irreparable harm through the loss of the information that Cox wrongfully removed from BILL. (Ex. A ¶ 8, 11-12.) BILL entrusted Cox with enhanced

access to its systems and networks and Cox abused that access to exfiltrate thousands of highly-sensitive emails from her colleagues, as well as the internal chat logs for BILL’s entire company for a nearly four-month period. (Ex. C ¶ 13.) Cox’s actions place BILL at significant risk of irreparable harm, both through the loss of its trade secrets and the loss of its goodwill with customers. (Ex. A ¶13.) Both the DTSA and UTSA expressly allow this Court to enter injunctive relief specifically to prevent this kind of harm. 18 U.S.C. § 1836(b)(3)(A), Utah Code § 13-24-3. BILL should not have to wait until Cox publishes its trade secrets, or gives them to a competitor, before obtaining injunctive relief protecting that information. Under these circumstances, BILL’s limited request for injunctive relief is appropriate and should be granted.

**C. The Balance of Hardships Weighs in Favor of BILL.**

The third preliminary injunction factor requires the court to “balance the irreparable harms [facing plaintiff if the injunction is denied] against the harm to defendants if the preliminary injunction is granted.” *Fish v. Kobach*, 840 F.3d 710, 754 (10th Cir. 2016). The Tenth Circuit has recognized that when the injunction would prevent a party from using or possessing property with “no real claim to ownership,” the potential harm to the defendant is minimal. *See RoDa Drilling Co. v. Siegal*, 552 F.3d 1203, 1214 (10th Cir. 2009) (affirming entry of preliminary injunction ordering defendant to return record title to plaintiff even under “heightened” injunction standard, and noting lack of any discernable harm to defendant considering lack of ownership); *see also Orbit Irr. Prod. v. Sunhills Int’l*, No. 1:10-CV-113 TS, 2015 WL 1393232, at \*8 (D. Utah Mar. 25, 2015) (balance of hardships favored the plaintiff where the defendant could not show appreciable hardship); *Orchard Sec., LLC v. Pavel*, No. 2:13-CV-00389-RJS, 2013 WL 4010228, at \*5 (D. Utah Aug. 6, 2013) (accord).

In this instance, as explained above, the irreparable harm that BILL faces in the absence of injunctive relief—the loss or disclosure of its confidential and trade secret information—vastly outweighs any potential harm to Cox if the injunction is granted. Indeed, it is difficult to imagine *what* harm would be visited upon Cox if BILL’s Motion were granted, considering the only relief that BILL seeks is what Cox is already required to do under the law and her contractual agreement: (1) not use or disclose BILL’s confidential and trade secret information, (2) return BILL’s data and equipment to it in a way that preserves relevant information, and (3) not destroy any relevant evidence. To be clear, BILL is specifically seeking an Order that requires Cox to return data to BILL through a third-party forensics vendor, so that any relevant metadata connected to that data will be preserved. Under similar circumstances, this Court has recognized the need for such procedures and ordered them to be employed. *See ClearOne Commc'ns, Inc. v. Chiang*, 608 F. Supp. 2d 1270, 1282 (D. Utah 2009), *aff'd in part sub nom. ClearOne Commc'ns, Inc. v. Bowers*, 643 F.3d 735 (10th Cir. 2011) (directing defendants to return misappropriated trade secrets to rightful owner “through use of a third-party forensic computer expert”).

When all that BILL is seeking is a return of property that Cox has no right to possess or use in the first place, Cox faces no harm at all from the requested injunction. *See RoDa Drilling Co.*, 552 F.3d at 1214. The balance of hardships weighs strongly in favor of BILL, and BILL’s Motion should be granted on these grounds.

**D. The Public Interest Favors a Temporary Restraining Order and Preliminary Injunction.**

Finally, BILL’s Motion should be granted because doing so would be in the public interest. Utah law and this Court have long recognized that the public has a strong interest in both protecting legitimate trade secrets and in maintaining the integrity of contracts. *Mountain Am. Credit Union*

*v. Godfrey*, 2006 U.S. Dist. LEXIS 52224, at \*10, 2006 WL 2129465 (D. Utah 2006) (finding that there “is a strong public interest in requiring adherence to contracts and statutes”); *Neways Inc. v. Mower*, 543 F. Supp. 2d 1277, 1290 (D. Utah 2008) (holding that “the public has an interest in fair competition and the enforcement of lawful contractual obligations”); *Ophir-Spiricon, LLC v. Mooney*, 2011 U.S. Dist. LEXIS 135608, at \*11, 2011 WL 5881766 (D. Utah 2011) (recognizing “the public interest in the enforcement of contracts and preventing the misappropriation of trade secrets”). Considering the extraordinarily limited nature of the relief that BILL seeks here—the return of data and equipment that does not belong to Cox and indisputably belongs to BILL—the public interest would be served by the enforcement of BILL’s contractual rights and the protection of its confidential and trade secret information. For that reason, and all those set forth herein, BILL’s motion should be granted.

#### **IV. CONCLUSION**

Wherefore, BILL respectfully requests that the Court grant this Motion and enter an Order granting BILL the following relief (a proposed Order is attached hereto as Exhibit D):

- A. Enjoining Defendant Danielle Cox and all parties in active concert or participation with her from using or disclosing any of BILL’s confidential, proprietary, and/or trade secret information;
- B. Ordering Defendant Danielle Cox and all parties in active concert or participation with her to return to BILL all originals and copies of all files, data, information, and/or documents that contain or relate to BILL’s confidential, proprietary, and trade secret information, including without limitation all electronic media, and directing that the return of such information shall be done through a third-party forensic computer expert in order to preserve relevant metadata;
- C. Ordering Defendant Danielle Cox to immediately return to BILL the laptop computer that BILL issued to her, without altering or deleting any of the data on that device;

- D. Ordering Defendant Danielle Cox and all parties in active concert or participation with her, to preserve all documents, data, and electronic information, and to produce for inspection and imaging by a third-party forensic computer expert all computers and other electronic storage devices and email accounts belonging to, under the control of, accessible to, or operated by Defendant Cox; and
- E. Awarding BILL such further relief as the Court deems necessary and just.

DATED: January 12, 2023	Respectfully submitted,  SEYFARTH SHAW LLP  By: <u>/s/ Mark A. Wagner</u>

SEYFARTH SHAW LLP  
Kevin J. Mahoney (SBN 6299398) (*pro hac vice pending*)  
kmahoney@seyfarth.com  
233 South Wacker Drive  
Suite 8000  
Chicago, Illinois 60606-6448  
Telephone: (312) 460-5000  
Facsimile: (312) 460-7000

Mark. A. Wagner (UT 06353)  
mawagner@seyfarth.com  
975 F St., N.W.  
Washington, DC 20004  
Telephone: (415) 732-1152

Attorneys for Plaintiff  
Bill.com, LLC

**CERTIFICATE OF SERVICE**

I hereby certify that on January 12, 2023, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system. I also certify that I have mailed by United States this document to the following non-CM/ECF participants via U.S. certified mail, and have also sent this documents to the following non-CM/ECF participants via overnight courier, and via email to the following addresses:

Danielle Cox  
4882 N. Nile Drive  
Lehi, UT 84043  
daniellecox0@gmail.com

/s/ Mark A. Wagner